ESERCIZIO – CONSEGNA 2

Strumenti necessari:

- Kali Linux per eseguire le scansioni
- Metasploitable come macchina target
- Wireshark per l'intercettazione dei pacchetti
- Excel o Word per la creazione dei report

Passaggi per le Scansioni con Nmap

1. Scansione TCP sulle Porte Well-Known

Una scansione TCP completa tenta di connettersi a tutte le porte specificate per verificare se sono aperte.

```
bash
Copia codice
nmap -p 1-1024 -sT 192.168.3.245
```

2. Scansione SYN sulle Porte Well-Known

Una scansione SYN (half-open) invia pacchetti SYN per vedere se le porte rispondono con SYN-ACK (indicando che sono aperte).

```
bash
Copia codice
nmap -p 1-1024 -sS 192.168.3.245
```

3. Scansione con Switch `-A` sulle Porte Well-Known

La scansione con l'opzione `-A` esegue la rilevazione della versione, lo script scanning, e il traceroute.

```
bash
Copia codice
nmap -p 1-1024 -A 192.168.3.245
```

Utilizzo di Wireshark per Intercettare le Richieste

1. **Apri Wireshark su Kali Linux:**
   - Seleziona l'interfaccia di rete corretta.
   - Inizia la cattura dei pacchetti.
2. **Esegui le Scansioni:**
   - Esegui le scansioni TCP e SYN utilizzando i comandi sopra descritti.
   - Osserva e cattura i pacchetti di rete durante le scansioni.
3. **Analisi delle Differenze:**
   - Scansione TCP: vedrai una sequenza completa di pacchetti TCP (SYN, SYN-ACK, ACK).
   - Scansione SYN: vedrai solo pacchetti SYN e SYN-ACK senza completare la connessione (mancanza di pacchetti ACK).

Creazione dei Report

Crea un report strutturato in Excel o Word per ogni tipo di scansione effettuata. Ogni report dovrebbe contenere le seguenti sezioni:

- **Fonte dello Scan:** Kali Linux IP
- **Target dello Scan:** Metasploitable IP
- **Tipo di Scan:** Scansione TCP, Scansione SYN, Scansione con `-A`
- **Risultati Ottenuti:** Numero e descrizione dei servizi trovati

Esempio di Tabella del Report

Fonte dello Scan: 192.168.3.1 (Kali Linux)
Target dello Scan: 192.168.3.245 (Metasploitable)

Tipo di Scan	Porte Scansionate	Servizi Trovati	Descrizione Servizi
Scansione TCP	1-1024	15	FTP (21), SSH (22), Telnet (23), HTTP (80), RPC (111), SMB (445), etc.
Scansione SYN	1-1024	15	FTP (21), SSH (22), Telnet (23), HTTP (80), RPC (111), SMB (445), etc.
Scansione con `-A`	1-1024	15	Dettagli sui servizi: versioni, script results, traceroute

1. **Avvia Wireshark** su Kali Linux:
   - Apri Wireshark.
   - Seleziona l'interfaccia di rete corretta.
   - Inizia la cattura dei pacchetti.
2. **Esegui la scansione TCP completa** su Kali Linux:

```
bash
Copia codice
nmap -p 1-1024 -sT 192.168.3.245
```

B. Scansione SYN sulle Porte Well-Known

1. **Avvia una nuova cattura** in Wireshark o continua con quella attuale.
2. **Esegui la scansione SYN** su Kali Linux:

```
bash
Copia codice
nmap -p 1-1024 -sS 192.168.3.245
```

C. Scansione con Switch `-A` sulle Porte Well-Known

1. **Avvia una nuova cattura** in Wireshark o continua con quella attuale.
2. **Esegui la scansione con l'opzione `-A`** su Kali Linux:

```
bash
Copia codice
nmap -p 1-1024 -A 192.168.3.245
```

4. Analizzare le Differenze con Wireshark

1. **Filtrare i Pacchetti** in Wireshark:
    - Filtra i pacchetti SYN con `tcp.flags.syn == 1`.
    - Filtra i pacchetti completi TCP con `tcp.flags.syn == 1 and tcp.flags.ack == 1`.
    - Filtra i pacchetti `-A` con `nmap` per vedere i dettagli della scansione avanzata.
2. **Confrontare le Scansioni**:
    - **Scansione TCP Completa**: Vedrai una sequenza completa di pacchetti TCP (SYN, SYN-ACK, ACK) per ogni porta aperta.
    - **Scansione SYN**: Vedrai pacchetti SYN e SYN-ACK senza il pacchetto ACK finale (half-open).
    - **Scansione `-A`**: Oltre ai pacchetti SYN e SYN-ACK, vedrai anche pacchetti che identificano le versioni dei servizi e altre informazioni dettagliate.

5. Creare i Report

Per ogni scansione effettuata, crea un report dettagliato includendo le seguenti informazioni:

- **Fonte dello Scan**: IP di Kali Linux
- **Target dello Scan**: IP di Metasploitable
- **Tipo di Scan**: Scansione TCP, Scansione SYN, Scansione con `-A`
- **Risultati Ottenuti**: Numero e descrizione dei servizi trovati

Esempio di Tabella del Report

Fonte dello Scan	Target dello Scan	Tipo di Scan	Porte Scansionate	Servizi Trovati	Descrizione Servizi
192.168.3.X (Kali)	192.168.3.245	Scansione TCP Completa	1-1024	15	FTP (21), SSH (22), Telnet (23), HTTP (80), RPC (111), SMB (445), etc.
192.168.3.X (Kali)	192.168.3.245	Scansione SYN	1-1024	15	FTP (21), SSH (22), Telnet (23), HTTP (80), RPC (111), SMB (445), etc.
192.168.3.X (Kali)	192.168.3.245	Scansione con `-A`	1-1024	15	Dettagli sui servizi: versioni dei servizi trovati, risultati degli script Nmap, traceroute